

DETAILED ACTION

1. This Office Action is directed towards the Applicant's response filed 1-29-09.

2. Claims 1-4, 6-14, and 19 are pending and have been examined.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Charles Leyes on 4-22-09.

IN THE CLAIMS: Please amend claims 9 and 10 as follows:

9. A computer-readable memory having computer-readable program code portions stored therein for directing a computer to function in a particular manner when used by the computer, the computer-readable program code portions comprising: a first portion to direct the computer to receive data comprising an encrypted message and a hashed key; a second portion to direct computer to parse said data; a third portion to direct computer to compare said received hashed key with a plurality of keys and to select a key having a hash matching said received hashed key; and a fourth portion to direct computer to decrypt said encrypted message with said matching key if a match was found and send a request for a key to a network entity if no matching key was found.

10. A computer program product comprising at least one computer- readable storage medium having computer-readable program code portions stored therein, the computer-readable program code portions comprising: a first executable portion for parsing received data comprising an encrypted message and a hashed key to derive said encrypted message and said hashed key; a second executable portion for comparing said received hashed key with a plurality of keys that are prestored by a receiving node to select a key having a hash matching said received hashed key; and a third executable portion for decrypting said encrypted message with said matching key if a match was found and sending a request for a key to a network entity if no matching key was found.

Allowable Subject Matter

4. Claims 1-4, 6-14, and 19 are allowed.

5. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field does not teach the combination of features of the claimed invention, particularly including:

As per independent claims 1, 6, 8, and 11: a message security method and system for implementing the method comprising wirelessly transmitting an encrypted message containing the key used to encrypt it to a plurality of receiving nodes, and subsequently removing at least one node from the plurality of receivers by transmitting a message that includes a NULL key with the message configured so that the node is instructed to replace the message encryption key with the NULL key such that the node is thereafter unable to decrypt a message encrypted with the original key.

As per independent claims 4, 9, and 10: a message security method and system for implementing the method comprising receiving an encrypted message containing a hashed version of the key used to encrypt the message, recovering the hashed key from the message, comparing the hashed key with a plurality of pre-established key hashes, and decrypting the message with a key whose hash matches the recovered key hash, and if no match is found subsequently requesting a key from a network entity.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably

accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Paul Callahan/
Art Unit 2437

/Matthew B Smithers/
Primary Examiner, Art Unit 2437